

USB-WLAN-Stick 150 Mbit

Bedienungsanleitung

PX-2573-675

INHALTSVERZEICHNIS





Kapitel 1 - Produktübersicht und Inbetriebnahme





IHR NEUER WLAN-STICK

Sehr geehrte Kunden,

vielen Dank für den Kauf dieses USB-WLAN-Sticks. Mit diesem WLAN-Stick aus dem Hause 7Links haben Sie die Möglichkeit, Ihren Computer drahtlos in Ihr WLAN-Netz zu integrieren und so mit Ihrem Notebook oder Ihrem Computer Zugriff auf das Internet zu haben, ohne lästige Kabel zu verlegen. Alternativ lassen sich auch andere Geräte wie z.B. Android-Geräte mit diesem Stick leicht und komfortabel mit Ihrem Netzwerk verbinden.
Bitte lesen Sie die Bedienungsanleitung und befolgen Sie die Hinweise und Tipps, damit Sie diesen WLAN-Stick optimal nutzen können.

Lieferumfang

- WLAN-Stick
- Treiber-CD
- Infoblatt

Systemvoraussetzungen

- USB 2.0
- Windows XP/7 (32 Bit und 64 Bit), Android 2.2



WICHTIGE HINWEISE ZU BEGINN

Sicherheitshinweise & Gewährleistung

- Diese Bedienungsanleitung dient dazu, Sie mit der Funktionsweise dieses Produktes vertraut zu machen. Bewahren Sie diese Anleitung daher stets gut auf, damit Sie jederzeit darauf zugreifen können.
- Sie erhalten bei Kauf dieses Produktes zwei Jahre Gewährleistung auf Defekt bei sachgemäßem Gebrauch. Bitte beachten Sie auch die allgemeinen Geschäftsbedingungen!
- Bitte verwenden Sie das Produkt nur in seiner bestimmungsgemäßen Art und Weise. Eine anderweitige Verwendung führt eventuell zu Beschädigungen am Produkt oder in der Umgebung des Produktes.
- Ein Umbauen oder Verändern des Produktes beeinträchtigt die Produktsicherheit. Achtung Verletzungsgefahr!
- Führen Sie Reparaturen nie selber aus!
- Behandeln Sie das Produkt sorgfältig. Es kann durch Stöße, Schläge oder Fall aus bereits geringer Höhe beschädigt werden.
- Halten Sie das Produkt fern von Feuchtigkeit und extremer Hitze.
- Tauchen Sie das Produkt niemals in Wasser oder andere Flüssigkeiten.
- Verwenden Sie Funkprodukte niemals in direkter Nähe von Personen mit elektronischen Herzschrittmachern!



ACHTUNG:
Es wird keine Haftung für Folgeschäden übernommen.
Technische Änderungen und Irrtümer vorbehalten!

Informationen zur Entsorgung von elektronischen Geräten

Ihr neues Produkt wurde mit größter Sorgfalt entwickelt und aus hochwertigen Komponenten gefertigt. Trotzdem muss das Produkt eines Tages entsorgt werden. Die durchgestrichene Mülltonne bedeutet, dass Ihr Produkt am Ende seiner Lebensdauer getrennt vom Hausmüll entsorgt werden muss. Bitte bringen Sie in Zukunft alle elektrischen oder elektronischen Geräte zu den eingerichteten kommunalen Sammelstellen in Ihrer Gemeinde. Diese nehmen Ihre Geräte entgegen und sorgen für eine ordnungsgemäße und umweltgerechte Verarbeitung. Dadurch verhindern Sie mögliche schädliche Auswirkungen auf Mensch und Umwelt, die sich durch unsachgemäße Handhabung von Produkten am Ende von deren Lebensdauer ergeben können. Genaue Informationen zur nächstgelegenen Sammelstelle erhalten Sie bei Ihrer Gemeinde.

Konformitätserklärung

Hiermit erklärt Pearl Agency GmbH, dass sich dieses Produkt PX-2573 in Übereinstimmung mit den grundlegenden Anforderungen der gängigen Richtlinien befindet.

PEARL Agency GmbH
PEARL-Str. 1-3
79426 Buggingen
Deutschland
18.02.2011

Die ausführliche Konformitätserklärung finden Sie unter www.pearl.de. Klicken Sie auf der linken Seite auf den Link **Support (FAQ, Treiber & Co.)**. Geben Sie anschließend im Suchfeld die Artikelnummer PX-2573 ein.



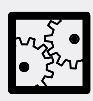




Hinweise zur Nutzung dieser Bedienungsanleitung

Um diese Bedienungsanleitung möglichst effektiv nutzen zu können, ist es notwendig vorab einige Begriffe und Symbole zu erläutern, die Ihnen im Verlauf dieser Anleitung begegnen werden.

Verwendete Symbole

	Dieses Symbol steht für mögliche Gefahren und wichtige Informationen im Umgang mit diesem Produkt. Es wird immer dann verwendet, wenn der Anwender eindringlich auf etwas hingewiesen werden soll.
	Dieses Symbol steht für nützliche Hinweise und Informationen, die im Umgang mit dem Produkt helfen sollen „Klippen zu umschiffen“ und „Hürden zu nehmen“.
	Dieses Symbol wird für beispielhafte Anwendungen und Erläuterungen verwendet, die oft komplexe Vorgehensweisen veranschaulichen und begreiflich machen sollen.
	Dieses Symbol wird oftmals hinter Fachbegriffen zu finden sein, zu denen weitere Erläuterungen im Glossar zu finden sind. Das Glossar soll dabei helfen, diese Fachbegriffe für den Laien verständlich zu machen und in einen Zusammenhang zu rücken.

Erläuterung der Navigationsschaltflächen

	Diese Schaltfläche leitet Sie von jedem Punkt des Dokuments aus zum angefügten Glossar weiter.
	Diese Schaltfläche leitet Sie von jedem Punkt des Dokuments aus zum Inhaltsverzeichnis zurück.

Verwendete Textmittel

GROSS-BUCHSTABEN	Großbuchstaben werden immer dann verwendet, wenn es gilt Tasten, Anschluss- oder andere Produkt-Beschriftungen kenntlich zu machen.
Fettschrift	Fettschrift wird immer dann eingesetzt, wenn Menüpunkte oder genau so bezeichnete Ausdrücke in der Software des Produktes verwendet werden.
1. Aufzählungen 2. Aufzählungen a. Aufzählungen	Aufzählungen werden immer dann verwendet, wenn der Anwender eine bestimmte Reihenfolge von Schritten befolgen soll, oder die Merkmale des Produktes beziffert werden sollen.
• Unterpunkte • Unterpunkte • Unterpunkte	Unterpunkte werden immer dann verwendet, wenn mehrere Informationen aufgelistet werden. Sie dienen hauptsächlich zum besseren kenntlich Machen der einzelnen Informationen.

VORBEREITUNG UND INBETRIEBNAHME

1. Packen Sie den WLAN-Stick vorsichtig aus.
2. Stecken Sie den WLAN-Stick in einen freien USB-Port Ihres Computers oder Android-Gerätes.



HINWEIS:
Android-Geräte erkennen diesen WLAN-Stick automatisch und er kann direkt genutzt werden. Beachten Sie dazu auch die Anleitung Ihres Android-Gerätes. Diese Anleitung befasst sich daher mit der Nutzung in Kombination mit einem Computer.

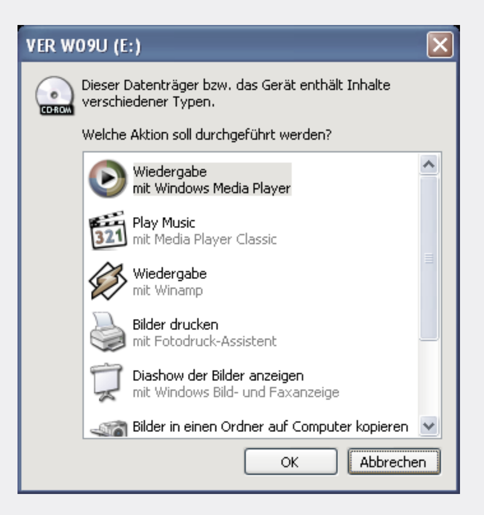
- Bei Windows XP und Vista wird der **Assistent für die Erkennung neuer Hardware** aktiviert.
- Brechen Sie die Hardwareinstallation von Windows ab.



ACHTUNG:
Unter Windows 7 wird der richtige Treiber direkt installiert. Daher können Sie die nächsten Kapitel direkt überspringen.

Installation unter Windows XP und Vista

Legen Sie die mitgelieferte Treiber-CD in ein freies Laufwerk Ihres Computers ein.
Brechen Sie den Wiedergabe-Dialog ab.



Öffnen Sie über Ihren Arbeitsplatz/Computer den CD-Inhalt und starten Sie das Installationsprogramm im **Windows Driver**-Unterverzeichnis.






EINRICHTEN EINER WLAN-VERBINDUNG

Nachdem die Installation der Treiber abgeschlossen wurde, kann direkt mit dem Einrichten einer Verbindung zu einem WLAN-Router oder Access-Point begonnen werden.

Windows XP

Öffnen Sie zuerst die Systemsteuerung. Dort wählen Sie die Auswahl **Netzwerkverbindungen**. Für die ordnungsgemäße Installation muss die drahtlose Netzwerkverbindung aktiviert werden. Mit der rechten Maustaste muss dafür auf die Verbindung geklickt und **Aktivieren** ausgewählt werden.
Nach der erfolgreichen Aktivierung klicken Sie doppelt auf die Netzwerkverbindung, es öffnet sich ein Fenster zur Auswahl der drahtlosen Netzwerkverbindungen. Erscheint keine Verbindung, muss **Netzwerkliste aktualisieren** angeklickt werden.

Erscheinen ein oder mehrere Verbindungen, wählen Sie die gewünschte aus. Mit einem Doppelklick verbinden Sie sich mit diesem Netzwerk.
Es erscheint eine Eingabeaufforderung, bei der der Netzwerkschlüssel eingegeben werden muss. Den Netzwerkschlüssel finden Sie in den Einstellungen des Routers oder er wird vom Systemadministrator (zum Beispiel in öffentlichen WLAN-Netzwerken) bekanntgegeben.

Wenn alle Eingaben korrekt waren, wird man mit dem WLAN-Netzwerk verbunden. Die Verbindung ist erfolgreich eingerichtet.

Windows 7

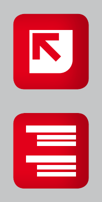
1. Zuerst öffnen Sie die Systemsteuerung.
2. Danach öffnen Sie das **Netzwerk- und Freigabecenter**. Dort sehen Sie, dass noch keine Verbindung zum Internet besteht. Zum Einrichten einer WLAN-Verbindung muss **Verbindung mit einem Netzwerk herstellen** gewählt werden.

   Im folgenden Fenster werden die verfügbaren WLAN-Netze in der Umgebung angezeigt. Neben dem Namen und Status finden Sie ein Balkendiagramm mit der Stärke des Netzwerkes. Je mehr Balken grün sind, desto besser ist das Netz. Mit der rechten Maustaste wählen Sie die entsprechende Verbindung und klicken danach auf die Auswahl **Verbindung herstellen**.

3. Nun fehlt nur noch die Eingabe des Sicherheitsschlüssels. Unbedingt zu beachten ist, dass der Netzwerkname nicht geändert wird. Der Sicherheitsschlüssel ist in den Routereinstellungen hinterlegt.

4. Stimmen alle Eingaben, wird die Verbindung erfolgreich eingerichtet und es erscheint ein Bildschirm, der mit **Schließen** beendet werden kann.

Kapitel 2 - Anhang

USB-PROBLEMLÖSUNGEN



HINWEIS:
Beim Anschluss von USB-Geräten an einen USB-Hub oder einen Switch kann ein auftretendes Problem von beiden Geräten verursacht worden sein. Sie sollten die folgenden Tipps zur Problemlösung daher soweit möglich immer sowohl am USB-Gerät selbst als auch an einem eventuellen Verbindungsgerät anwenden.

Das USB-Gerät wird nicht erkannt

- Überprüfen Sie, ob das Gerät eingeschaltet ist.
- Überprüfen Sie, ob Ihr Computer die Systemvorausetzungen (s. Seite 4) für das Gerät erfüllt.
- Trennen Sie das Gerät von Ihrem Computer. Starten Sie Ihr Betriebssystem neu und schließen Sie das Gerät erneut an.
- Wenn das Gerät an einen USB-Hub angeschlossen ist, schließen Sie es stattdessen direkt an Ihren Computer an.
- Überprüfen Sie, ob die passenden Gerätetreiber installiert sind.
- Die USB-Ports an der Vorderseite eines PCs liefern häufig nicht genug Strom oder sind sogar ganz außer Funktion. Trennen Sie das Gerät und schließen Sie es direkt an einen der USB-Ports an der Rückseite Ihres PCs an.
- Sollten Sie eine PCI-Karte mit zusätzlichen USB-Ports verwenden, schließen Sie das Gerät direkt an einen der USB-Ports Ihres Motherboards an.
- Versichern Sie sich, dass Sie das Gerät in denselben USB-Port eingesteckt haben wie bei der Installation der Gerätetreiber.
- Deinstallieren Sie die Gerätetreiber und installieren Sie diese neu.
- Überprüfen Sie, ob der USB-Port Ihres Computers funktioniert.
- Überprüfen Sie, ob die USB-Ports in den BIOS-Einstellungen Ihres Computers aktiviert sind.
- Sollten Ihre BIOS-Einstellungen die Legacy-USB Funktion haben, so deaktivieren Sie diese.
- Windows schaltet angeschlossene USB-Geräte nach längerer Inaktivität auf Energiesparmodus. Schließen Sie das Gerät erneut an oder schalten Sie die Energiesparfunktion aus. Klicken Sie hierfür rechts auf **Arbeitsplatz** und wählen Sie **Verwalten**. Klicken Sie auf **Geräte-Manager** ➡ **USB-Controller** ➡ **USB-Root-Hub**. Wählen Sie **Energieverwaltung** und entfernen Sie den Haken im oberen Feld.
- Windows XP erkennt die USB-Ports von Motherboards mit dem AMD 754 Chipsatz in vielen Fällen nicht. Installieren Sie in diesem Fall die **Bus Master Drivers** oder wenden Sie sich direkt an den Kundenservice des Herstellers.

Windows versucht das Gerät jedes Mal, wenn es angeschlossen wird, neu zu installieren.

Überprüfen Sie, ob die passenden Gerätetreiber installiert sind.
Versichern Sie sich, dass Sie das Gerät in denselben USB-Port eingesteckt haben, den Sie auch bei der Installation verwendet haben.
Löschen Sie die Gerätetreiber und installieren Sie diese neu.

Der Computer startet zu langsam oder überhaupt nicht mehr.

Je mehr USB-Geräte an Ihren Computer angeschlossen sind, desto länger wird das Betriebssystem zum Starten benötigen. Schließen Sie USB-Geräte erst an, nachdem der Computer hochgefahren wurde. Nicht benötigte USB-Geräte sollten vom Computer getrennt werden.

BASISWISSEN NETZWERKE

Da bei Netzwerken häufig Unklarheiten und missverständliche Begriffe auftreten, soll dieses Glossar dabei helfen, Licht ins Dunkel mancher Fachbegriffe zu bringen. Im Folgenden werden die grundlegenden Hardwarekomponenten eines herkömmlichen Heimnetzwerks ebenso dargestellt, als auch die verwendeten Anwendungen und Dienste.

Hardware

Access-Point
Der Zugangspunkt oder auch Access-Point ist die „Basisstation" in einem drahtlosen Netzwerk (WLAN). Diese Funktion wird häufig in Heimnetzwerken auch von einem Router übernommen.

DSL-Modem
Das DSL-Modem verbindet Ihren Computer mit dem Internet. Wenn Sie mit mehr als einem Computer über eine Leitung Zugriff auf das Internet haben wollen, benötigen Sie einen Router, der direkt hinter das DSL-Modem geschalten wird.

Kabelmodem
Als Kabelmodem bezeichnet man das Gerät, das Daten über Fernseh-Kabelnetze überträgt und für Breitband-Internetzugänge über Kabelanschlüsse (Kabelinternet) eingesetzt wird.

Netzwerkhub
Netzwerkhubs wurden in der Vergangenheit als „Knotenpunkt" verwendet, um mehrere Netzwerkgeräte miteinander zu verbinden. Jedoch wurden Sie inzwischen weitestgehend durch Netzwerkswitches abgelöst.

Netzwerkkabel/Ethernetkabel
Hier gibt es zwei Varianten: So genannte „Patch"-Kabel und „Crossover"-Kabel. Patchkabel sind die Kabel, die am häufigsten Verwendung in Netzwerken finden. Sie werden eingesetzt um Computer mit Switches, Hubs oder Routern zu verbinden. Crossover-Kabel werden dazu eingesetzt um zwei Computer direkt miteinander zu verbinden, ohne ein Netzwerk zu verwenden. Patchkabel sind der gängige Lieferumfang von Netzwerkprodukten.

Netzwerkkarten
Netzwerkkarten werden in der heutigen Zeit oftmals schon auf den Hauptplatinen (Mainboards) integriert. Die Anschlüsse ähneln denen von Telefonanschlüssen. Der Stecker hierzu hat die technische Bezeichnung RJ-45. Sie dienen zur Datenübertragung an ein Netzwerk.

Netzwerkswitch
Switches werden als „Knotenpunkt" von Netzwerken eingesetzt. Sie dienen dazu, mehrere Netzwerkgeräte „auf ein Kabel" im Netzwerk zusammenzuführen. Switches sind häufig zu logischen Verbünden zusammengestellt und verbinden z.B. alle Computer aus einem Büro. Koppelt man mehrere Switches, erhält man ein komplexeres Netzwerk, welches einer Baumstruktur ähnelt.

Router
Router dienen zur Zugriffssteuerung von Netzwerkcomputern untereinander und regeln ebenfalls den Zugriff auf das Internet für alle sich im Netzwerk befindlichen Computer. Router werden sowohl rein kabelgebunden als auch als WLAN-fähige Variante vertrieben. Meist übernehmen handelsübliche Router noch Sonderfunktionen wie z.B. DHCP, QoS, Firewall, NTP,…

WLAN-Karten und WLAN-Dongles
Zunehmend werden drahtlose Netzwerke eingesetzt, so genannte WLANs. Um eine Verbindung zu einem WLAN herstellen zu können, wird eine spezielle Hardware benötigt. Diese Hardware existiert häufig in Form von WLAN-Karten oder WLAN-Dongles (-Sticks). WLAN-Karten werden in Desktop-Computern („normaler" Computer) verwendet, während WLAN-Dongles häufig für den mobilen Einsatz gedacht sind (Notebooks) und werden über USB betrieben.

Grundlegende Netzwerkbegriffe

Adressbereich
Ein Adressbereich ist eine festgelegte Gruppe von IP- oder MAC-Adressen und fasst diese zu einer „Verwaltungseinheit" zusammen.

Blacklist
Mit einer Blacklist bezeichnet man bei Netzwerken eine Liste von Geräten, denen die Verbindung zu einem Gerät (z.B. Router) explizit nicht erlaubt ist. Alle anderen Geräte werden von dem Gerät akzeptiert, das den Zugang über die Blacklist regelt. Im Gegensatz dazu steht die so genannte Whitelist.

Browser
Browser werden Programme genannt die hauptsächlich zur Darstellung von Webseiten genutzt werden. Die bekanntesten Browser sind mitunter der Internet Explorer, Mozilla Firefox, Opera oder Google Chrome.

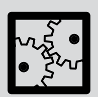
Client
Als Client wird jede Anwendung bezeichnet, die Daten eines Serverdienstes in Anspruch nimmt. Eine klassische Client-Server-Bindung entsteht in Heimnetzwerken häufig schon bei der Vergabe von IP-Adressen im Netzwerk. Hier fordert der Computer als DHCP-Client eine gültige IP-Adresse vom DHCP-Server (meist der Router) an und erhält diese vom DHCP-Server zugeteilt.

Flood Protection
Dieser Begriff umschreibt einem Schutzmechanismus von Servern oder Routern, der diese gegen massive Anhäufungen von Anfragen von außen schützt. Der Vergleich eines Damms, der Land gegen Überflutungen schützt, gibt dieser Technik Ihre englische Bezeichnung.



OSI-Schichtenmodell (Aufbau von Netzwerken)
Das OSI-Schichtenmodell dient zur Veranschaulichung der in Netzwerken verwendeten Protokolle. Jede Ebene dieser Modelle baut auf den darunter liegenden Ebenen auf. So ist z.B. einem Gerät eine MAC-Adresse zugeordnet, aber keine IP-Adresse (bei Switches); jedoch ist einem Gerät mit einer IP-Adresse IMMER auch eine MAC-Adresse zugeordnet.

IP-Adresse
IP-Adressen werden dazu verwendet, Computer, Drucker oder andere Geräte flexibel in ein Netzwerk einzubinden. Hierbei ist zwischen globalen und privaten IP-Adressen zu unterscheiden. Globale IP-Adressen werden von den einzelnen Internet-Anbietern oftmals dynamisch (DHCP) vergeben. Sie dienen dazu, Ihr Heimnetzwerk oder auch nur den einzelnen Computer gegenüber dem Internet erreichbar zu machen. Private IP-Adressen werden im Heimnetzwerk entweder statisch („von Hand" zugewiesen) oder dynamisch (DHCP) vom Anwender selbst vergeben. IP-Adressen ordnen ein spezielles Gerät eindeutig einem bestimmten Netzwerk zu.



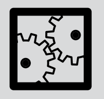
BEISPIEL:
IP-Adressen sind die bekanntesten Adressierungen im Netzwerk und treten in folgender Form auf: z.B. 192.168.0.1.

ISP
ISP ist die Abkürzung für „Internet Service Provider". Dieser Begriff wird für Stellen verwendet, die einem Netzwerk oder Einzelcomputer den Zugang zum Internet anbieten. In Deutschland ist der wohl bekannteste ISP T-Online, aber auch Anbieter wie Freenet, Arcor, 1&1 oder Kabel-Deutschland gehören zu den ISPs.

LAN
LAN (Local Area Network) bezeichnet ein Netzwerk aus Computern und anderen Netzwerkgeräten, die über einen gemeinsamen Adressbereich verfügen und damit zu einer Struktur zusammengefasst werden.

Passphrase
Mit dem Begriff Passphrase wird ein Schlüsselwort oder Satz umschrieben, der als Sicherheitsabfrage bei der Verbindung zu WPA-/WPA2-Verschlüsselten Netzwerken eingegeben werden muss.

Port
Als Port wird eine Softwareschnittstelle bezeichnet, die es einzelnen Anwendungen auf Ihrem Computer ermöglicht, mit den Anwendungen eines Anbieters zu kommunizieren. Hier wird hauptsächlich zwischen zwei Protokollen unterschieden:
TCP und UDP.



BEISPIEL:
Die häufigste Internet-Anwendung ist ein Browser (Internet Explorer, Mozilla Firefox, usw.), welcher meist über den TCP-Port 80 mit den Servern der Webseiten-Anbieter kommuniziert.

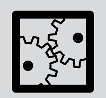
POE
Power over Ethernet (PoE) bezeichnet ein Verfahren, mit dem netzwerkfähige Geräte über das Ethernet-Kabel mit Strom versorgt werden können.

Protokoll
Protokolle im Netzwerk sind Standards für Datenpakete, die Netzwerkgeräte untereinander austauschen, um eine eindeutige Kommunikation zu ermöglichen.

Pre-Shared Key
Mit Pre-Shared Key („vorher vereinbarter Schlüssel") oder kurz PSK bezeichnet man ein Verschlüsselungsverfahren, bei denen die verwendeten Schlüssel vor der Verbindung beiden Teilnehmern bekannt sein muss (siehe auch WPA/WPA2).



MAC-Adresse
Als MAC-Adresse bezeichnet man die physikalische Adresse einer Netzwerkkomponente (z.B. Netzwerkkarte, WLAN-Dongle, Drucker, Switch). MAC-Adressen sind entgegen IP-Adressen immer eindeutig zuordenbar. MAC-Adressen von anderen verbundenen Netzwerkgeräten werden von den einzelnen Geräten jeweils in einer so genannten ARP-Tabelle gespeichert. Diese ARP-Tabellen können zur Fehlersuche dienen, falls ein Gerät ohne IP-Adresse (z.B. Switch) im Netzwerk keine Funktion zeigt.



BEISPIEL:
Eine MAC-Adresse sieht z.B. so aus: 00:00:C0:5A:42:C1

Sichere Passwörter
Unter sicheren Passwörtern versteht man Passwörter, die bestimmte Bedingungen erfüllen, um von Angreifern nicht mit einfachsten Mitteln entschlüsselt werden zu können.
Sichere Passwörter sollten generell eine bestimmte Mindestlänge aufweisen und mehrere Sonderzeichen beinhalten. Als Faustregel gilt hier: Je länger das Passwort ist und je mehr Sonderzeichen es beinhaltet, desto sicherer ist es gegen Entschlüsselung.

SSID
SSID (Service Set Identifier) steht für die Bezeichnung, die für ein WLAN-Netzwerk verwendet wird. Diese SSID wird meist per Broadcast (siehe UDP) öffentlich ausgesendet, um das Netzwerk für mobile Geräte „sichtbar" zu machen.

Subnetz
Subnetze sind eine Zusammenfassung von einzelnen IP-Adressen zu Netzwerkstrukturen. So werden meist Computer einer Abteilung im Büro in einem Subnetz zusammengefasst, während die Computer einer anderen Abteilung in einem weiteren Subnetz zusammengefasst sind. Daher sind Subnetze eine reine Strukturierungsmaßnahme. Eine Angabe des Subnetzraumes wird immer in Zusammenhang mit der Vergabe einer IP-Adresse durchgeführt. Im Heimbereich werden normalerweise keine speziellen Subnetze eingerichtet. Daher ist bei Windows-Systemen als Subnetzmaske die 255.255.255.0 voreingestellt. Dadurch stehen die IP-Adressen xxx.xxx.xxx.1 bis xxx.xxx.xxx.254 zur Verfügung.

TCP (Transmission Control Protocol)
Das TCP-Protokoll wird dazu verwendet, gezielt Informationen von einem speziellen Gegenüber abzufragen (siehe Beispiel bei Port)

Traffic
Mit Traffic bezeichnet man die ausgetauschten Datenmengen zwischen zwei Stellen oder aber auch den gesamten Datenverkehr in einem Netzwerkabschnitt.

UDP (User Datagram Protocol)
Das UDP-Protokoll ist ein so genanntes „Broadcast"-Protokoll. Broadcast wird im englischen auch für Radio- oder TV-Sendungen verwendet. Ganz ähnlich arbeitet dieses Protokoll. Es wird verwendet, um Datenpakete an alle im Netzwerk erreichbaren Geräte zu senden und im Weiteren auf Rückmeldung dieser Geräte zu warten. Das UDP-Protokoll wird meist dann von Anwendungen eingesetzt, wenn unsicher ist, ob eine entsprechende Gegenstelle im Netzwerk vorhanden ist.

uPNP
Mit diesem Begriff wird das „universal Plug and Play"-Protokoll bezeichnet. Dieses Protokoll wird hauptsächlich dazu verwendet, Drucker und ähnliche Peripheriegeräte über ein Netzwerk ansteuern zu können.

Verschlüsselung
Verschlüsselungsmechanismen werden in Netzwerken dazu eingesetzt, Ihre Daten vor fremdem Zugriff abzusichern. Diese Verschlüsselungsmechanismen funktionieren ähnlich wie bei einer EC-Karte. Nur mit dem richtigen Passwort (der richtigen PIN) können die Daten entschlüsselt werden.





VPN
VPN (Virtual Private Network) steht für eine Schnittstelle in einem Netzwerk, die es ermöglicht, Geräte an ein benachbartes Netz zu binden, ohne dass die Netzwerke zueinander kompatibel sein müssen.

WAN
WAN (Wide Area Network) bezeichnet ein Netzwerk aus Computern und anderen Netzwerkgeräten, die über größere Entfernungen und aus vielen Bestandteilen zusammengefasst werden. Das bekannteste Beispiel ist das „Internet“, jedoch kann ein WAN auch nur aus zwei räumlich voneinander getrennten LANs bestehen.

Whitelist
Mit einer Whitelist bezeichnet man bei Netzwerken eine Liste von Geräten, denen die Verbindung zu einem Gerät (z.B. Router) explizit erlaubt ist. Alle anderen Geräte werden von dem Gerät abgewiesen, das den Zugang über die Whitelist regelt. Im Gegensatz dazu steht die so genannte Blacklist.

Dienste in Netzwerken

DHCP (Dynamic Host Configuration Protocol)
Mit DHCP wird die dynamische Verteilung von IP-Adressen in Netzwerken bezeichnet. Dynamisch sind diese Adressen deshalb, weil sie jederzeit ohne größeren Aufwand neu vergeben werden können. Man kann dynamische IP-Adressen auch als geliehene IP-Adressen bezeichnen. Diese geliehenen IP-Adressen werden mit einem „Verfallsdatum“ versehen – der so genannten „Lease Time“. Ein Computer wird am DHCP-Server nur dann nach einer neuen IP-Adresse anfragen, wenn sein „Lease“ abgelaufen ist. Dies ist allerdings auch eine mögliche Fehlerquelle, da es hier zu Unstimmigkeiten zwischen DHCP-Server und DHCP-Clients kommen kann.



HINWEIS:
Windows Computer sind standardmäßig als DHCP-Client eingestellt, um einen einfachen Anschluss an ein Heimnetzwerk zu ermöglichen.

DNS (Domain Name Server)
DNS ist ein Serverdienst, der die Übersetzung von IP-Adressen in gängige Internet-Adressen übernimmt. So wird z.B. aus www.google.de die IP-Adresse: 74.125.39.105. Werden Sie während einer Konfiguration aufgefordert, die DNS-IP-Adresse einzugeben, ist damit immer die Adresse desjenigen Servers gesucht, welcher den DNS-Serverdienst anbietet. DNS-Server werden aus Gründen der Ausfallsicherheit meist doppelt angegeben und als Primärer DNS (oder DNS1), bzw. Sekundärer DNS (oder DNS2) bezeichnet.

Filter
Siehe auch Firewall

Firewall

Eine Firewall ist ein Sicherungsmechanismus, welcher meist auf Routern  als Serverdienst läuft, jedoch bereits in Windows (seit XP) integriert ist. Sie erlaubt nur Zugriffe auf voreingestellte Ports, blockt vorher konfigurierte IP-Adressen und soll generell schädliche Angriffe auf Ihr Netzwerk verhindern.

FTP/NAS (File Transfer Protocol/ Network Access Storage)

FTP ist ein Serverdienst, der hauptsächlich zum Transfer von Dateien verwendet wird. Dieser Dienst ermöglicht es auf unkomplizierte Art und Weise, Dateien von einem Computer auf einen entfernt stehenden anderen Computer ähnlich dem Windows Explorer zu übertragen. So genannte NAS-Server setzen ebenfalls häufig diesen Dienst ein, um einen Zugriff aus dem gesamten Netzwerk auf eine Festplatte zu erlauben.

(Standard-) Gateway

Als Gateway wird die Schnittstelle bezeichnet, die es den Computern im privaten Netzwerk ermöglicht, mit Computern außerhalb zu kommunizieren. Es ist in diesem Sinne mit Ihrem Router gleichzusetzen. Das Gateway sammelt und sendet Anfragen der Clients und leitet diese weiter an die entsprechenden Server im Internet. Ebenso verteilt das Gateway die Antworten der Server wieder an die Clients, die die Anfrage gestellt hatten.

HTTP/Webserver (Hypertext Transfer Protocol)

Dieser Dienst ist das, was in der Öffentlichkeit als „Das Internet" bezeichnet wird, jedoch handelt es sich hier bei nur um eine Vereinfachung, da das Internet an sich eine übergeordnete Struktur ist, welche nahezu alle Serverdienste beinhaltet. HTTP wird zum Transfer und der Darstellung von Webseiten verwendet.

Mediastreams

Diese Gruppe von Serverdiensten wird von vielfältigen Geräten und Anbietern verwendet. Die bekanntesten Beispiele sind Internet-Radiosender, Video-On-Demand und IP-Kameras. Diese Streams nutzen teils unterschiedliche Protokolle und Protokollversionen. Daher kann es hier durchaus einmal zu Inkompatibilitäten zwischen Server und Client kommen.

NTP

NTP (Network Time Protcol) bezeichnet ein Protokoll, mit dem Computer über das Netzwerk Ihre Datums- und Zeiteinstellungen abgleichen können. Dieser Dienst wird von weltweit verteilten Servern bereitgestellt.

PPPoE

PPPoE steht für PPP over Ethernet und bezeichnet Verwendung des Netzwerkprotokolls Point-to-Point Protocol (PPP) über eine Ethernet-Verbindung. PPPoE wird in Deutschland hauptsächlich in Verbindung mit ADSL-Anschlüssen verwendet. ADSL bedeutet Asynchrones DSL und steht für die Verwendung einer Leitung für Telefon und Internet. ADSL ist Standard in Deutschland.

Hauptgrund für die Verwendung von PPPoE ist die Möglichkeit, Authentifizierung und Netzwerkkonfiguration (IP-Adresse, Gateway) auf dem schnelleren Ethernet zur Verfügung zu stellen.

QoS (Quality of Service)

QoS wird in Netzwerken dazu verwendet, für bestimmte Clients oder Dienste eine bestimmte, garantierte Bandbreite für den Datenverkehr zu gewährleisten. Als Vergleich lässt sich eine Autobahn heranziehen, auf der selbst bei einem Stau die Standspur von Rettungsfahrzeugen genutzt werden kann, um voranzukommen. QoS wird also immer dann verwendet, wenn sichergestellt werden soll, dass bestimmte Dienste immer verfügbar sein sollen – ohne dabei auf den restlichen Datenverkehr Rücksicht nehmen zu müssen.

Samba/SMB

Mit diesen Begriffen ist ein Serverdienst gemeint, der speziell in Windows-Netzwerken verwendet wird. Dieser Service ermöglicht ebenfalls den schnellen und einfachen Zugriff auf Dateien, die sich auf anderen Computern befinden (in so genannten „freigegebenen Ordnern"). Jedoch ist dieser Dienst auf Heimnetzwerke begrenzt und kann nur in Ausnahmefällen auch über das Internet in Anspruch genommen werden.





Server/Serverdienst
Ein Server ist immer als Anbieter von Netzwerkdiensten zu sehen. Einzelne Anwendungen werden auch als Serverdienst bezeichnet. Die bekanntesten Serverdienste sind unter anderem Webserver, DHCP oder E-Mail Server. Mehrere solche Dienste können auf einem Computer oder anderen Geräten (z.B. Routern) gleichzeitig verfügbar sein. Server werden auch Computer genannt, deren ausschließliche Funktion darin besteht, Serverdienste anzubieten und zu verwalten.

Statische Adressvergabe
Bei der statischen Adressvergabe sind alle Netzwerkadressen eines Netzwerkes fest vergeben. Jeder einzelne Client (Computer) des Netzwerks hat seine feste IP-Adresse, die Subnetzmaske, das Standard-Gateway und den DNS-Server fest eingespeichert und muss sich mit diesen Daten beim Server anmelden. Ein neuer Client (Computer) muss erst mit einer gültigen, noch nicht vergebenen IP-Adresse und den restlichen Daten ausgestattet werden, bevor er das Netzwerk nutzen kann. Manuelle Adressvergabe ist besonders bei Netzwerkdruckern oder ähnlichen Geräten sinnvoll, auf die häufig zugegriffen werden muss, oder in Netzwerken, die besonders sicher sein müssen.

WEP und WPA
Wired Equivalent Privacy (WEP) ist der ehemalige Standard-Verschlüsselungsalgorithmus für WLAN. Er soll sowohl den Zugang zum Netz regeln, als auch die Vertraulichkeit der Daten sicherstellen. Aufgrund verschiedener Schwachstellen wird das Verfahren als unsicher angesehen. Daher sollten WLAN-Installationen die sicherere WPA-Verschlüsselung verwenden.
Wi-Fi Protected Access (WPA) ist eine modernere Verschlüsselungsmethode für ein WLAN. Sie wurde als Nachfolger von WEP eingeführt und weist nicht deren Schwachstellen auf.

Sicherheitsmaßnahmen in WLAN-Netzwerken

An erster Stelle sollten der Verzicht von WEP und der Einsatz von WPA oder WPA2 stehen. Dieses Ziel lässt sich in vielen Fällen bereits durch ein Treiber- oder Firmwareupdate erreichen. Lässt sich der Einsatz von WEP nicht vermeiden, sollten folgende grundlegende Behelfsmaßnahmen beachtet werden, um das Risiko von Angriffen fremder Personen auf das WLAN zu minimieren:

- Aktivieren Sie auf alle Fälle den Passwortschutz! Ändern Sie ggf. das Standard-Passwort des Access-Points.
- Wenn Sie die WEP-Verschlüsselung verwenden, weil eines der angeschlossenen Geräte WPA oder WPA2 (dringend empfohlen) nicht unterstützt, sollte der WEP-Schlüssel mindestens 128 Bit lang sein und eine lose Kombination aus Buchstaben, Ziffern und Sonderzeichen darstellen.
- Aktivieren Sie die Zugriffskontrollliste (ACL = Access Control List), um vom Access Point nur Endgeräte mit bekannter MAC-Adresse zuzulassen. Beachten Sie, dass sich eine MAC-Adresse aber mittels Treiber beliebig einstellen lässt, sodass eine mitgelesene zugelassene MAC-Adresse leicht als eigene ausgegeben werden kann.
- Verwenden Sie eine sinnvolle SSID: Die SSID des Access-Points sollte keine Rückschlüsse auf Ihren Namen, verwendete Hardware, Einsatzzweck und Einsatzort zulassen.
- Umstritten ist die Deaktivierung der SSID-Übermittlung (Broadcasting). Sie verhindert das unabsichtliche Einbuchen in das WLAN, jedoch kann die SSID bei deaktiviertem Broadcasting mit einem so genannten Sniffer (Gerät zur LAN-Analyse) mitgelesen werden, wenn sich etwa ein Endgerät beim Access-Point anmeldet.
- WLAN-Geräte (wie der Access-Point) sollten nicht per WLAN konfiguriert werden, sondern ausschließlich über eine kabelgebundene Verbindung.
- Schalten Sie WLAN-Geräte stets aus, wenn Sie sie nicht benutzen.
- Führen Sie regelmäßige Firmware-Updates vom Access Point durch, um sicherheitsrelevante Aktualisierungen zu erhalten.
- Reichweite des WLANs durch Reduzierung der Sendeleistung bzw. Standortwahl des WLAN Gerätes beeinflussen (Dies dient allerdings nicht der aktiven Sicherheit, sondern begrenzt lediglich den möglichen Angriffsbereich.)



Alle diese Sicherheitsmaßnahmen dürfen aber nicht darüber hinweg-täuschen, dass diese letztlich keinen wirklichen Schutz beim Einsatz von WEP bedeuten. Ein Angriff auf die WEP-Verschlüsselung ist trotz all dieser Vorkehrungen mit den richtigen technischen Voraussetzungen innerhalb von 5 bis 10 Minuten mit ziemlicher Sicherheit erfolgreich.




TECHNISCHE DATEN

Antenne	2 dbi
Standard	IEEE 802.11g/b/n
Frequenzband	2,412GHz - 2,4835GHz
Arbeitstempe-ratur	0 °C - 50 °C
Übertra-gungstyp	IEEE 802.11g: OFDM(64-QAM, 16-QAM, QPSK, BPSK) IEEE 802.11b: DSSS(CCK/DQPSK/DBPSK) IEEE 802.11n: MIMO-OFDM-BPSK/QPSK/QAM
Datenrate	802.11g: 54, 48, 36, 24, 18, 12, 9 & 6 Mbps 802.11b: 11, 5.5, 2 und 1 Mbps 802.11n: max. 150 Mbps
Betriebsluft-feuchtigkeit	10% - 90% (nicht kondensierend)
Sicherheit	64/128bit WEP WPA(TKIP mit IEEE 802.1x) WPA2(AES mit IEEE 802.1x)

